Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 21 février 2002
N° CERTA-2002-AVI-040

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft SQL Server 7.0 et 2000

Gestion du document

Référence	CERTA-2002-AVI-040
Titre	Vulnérabilité dans Microsoft SQL Server 7.0 et 2000
Date de la première version	21 février 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS02-007
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Coupure du service `MSSQLSERVER` ;
- prise de contrôle de la base SQL ;
- exécution de code arbitraire.

2 Systèmes affectés

- Microsoft SQL Server 7.0 ;
- Microsoft SQL Server 2000.

3 Résumé

Un utilisateur mal intentionné peut arrêter le service `MSSQLSERVER`, prendre possession de la base, installer et exécuter du code arbitraire.

4 Description

L'interface OLE DB peut être connectée à une source de données distante par le biais d'une connexion « ad hoc » (utilisée pour les connexions peu fréquentes). Un débordement de mémoire peut arriver lors de l'utilisation des fonctions associées à ce type de connexion.

L'exploitation de cette vulnérabilité des serveurs SQL Microsoft peut permettre à un utilisateur mal intentionné d'arrêter le service `MSSQLSERVER`, de prendre possession de la base ou bien d'exécuter du code arbitraire à distance. Les effets de cette vulnérabilité dépendent du contexte de sécurité dans lequel le service `MSSQLSERVER` a été lancé.

5 Solution

Appliquer le correctif fournit par Microsoft suivant la version:

- SQL Server 7.0:
  http://support.microsoft.com/support/misc/kblookup.asp?id=Q318268
- SQL Server 2000:
  http://support.microsoft.com/support/misc/kblookup.asp?=id=Q316333

6 Documentation

Bulletin de sécurité MS02-007 de Microsoft :
http://www.microsoft.com/technet/security/bulletin/ms02-007.asp

Gestion détaillée du document

21 février 2002 version initiale.